SOLUTION BRIEF

proofpoint.

PROOFPOINT CLOUD APP SECURITY

PROTECT YOUR CLOUD USERS. PROTECT YOUR DATA.

CHALLENGES

- Compromised credentials
- Malware
- Data loss and compliance risks

KEY CAPABILITIES

- Protect users and data from account compromise and advanced threats in the cloud
- Integrate threat detection and access controls across email and cloud
- Control cloud access with user behaviour analytics and multi-factor authentication (MFA)
- Protect against data loss with integrated threat insights
- Control third-party add-on apps
- Deploy quickly in the cloud

PRODUCTS

- Targeted Attack Protection (TAP)
- Cloud App Security Broker (PCASB)
- Email Data Loss Prevention and Encryption

Protecting your people and the data they create is more challenging—and critical—than ever.

That's because users, apps and data no longer sit behind your network perimeter. Users work from home, a coffee shop or on a train using cloud-based email and apps such as Microsoft Office 365, Google G Suite, and Box. These apps contain sensitive data and connect to a wide range of third-party add-ons.

At the same time, today's cyber attacks target people, not just infrastructure. Many focus on specific people or companies. They're crafted to emulate the way you work. And they trick people into opening unsafe files, clicking on malicious web links, and installing risky add-ons. The result: compromised credentials, malware run amok, data loss and compliance issues.

The path to better security lies in an integrated approach that puts people at the centre. To secure your move to the cloud, you need threat detection, access controls and data security. And they must work across all the cloud-based email and productivity tools you use.

Proofpoint Cloud App Security protects against account compromise, malicious files, data loss and compliance risks in the cloud. Our complete, people-centric solution helps secure email, storage, collaboration apps and more. It combines these key capabilities:

- Advanced threat protection against malicious files
- Compromised account detection and response
- Access controls for users and third-party apps
- Data loss prevention (DLP)
- Analytics and multifactor authentication

With these powerful features, you can defend against targeted attacks. You can safeguard your information. And you can stay compliant in the cloud.

PROTECT CLOUD USERS FROM ADVANCED THREATS

As users migrate to the cloud, so do cyber attacks. Ransomware, banking Trojans, credential stealers and credential phishing—these are just a few of the advanced threats that target people through email and other cloud apps.

A malicious document uploaded to a cloud drive can spread instantly throughout your environment through enterprise file sync and share (EFSS). That's why early detection matters. But polymorphic malware and malicious links (each with many variants) can be hard to detect with legacy tools.

Cloud App Security detects, analyses and blocks malicious files and URLs. It uses a blend of sandboxing, threat intelligence and cross-channel threat correlation to spot hidden threats and stop them.

Sandboxing

Our sandboxing and predictive analytics stop threats quickly and accurately—before they cause lasting harm. The entire attack chain is inspected using static and dynamic techniques. We observe behaviour, code and protocol to identify malicious files.

Our technology not only detects attacks, but also learns from them. It observes the patterns, behaviours and tradecraft used in each attack, making the next one easier to catch. It helps you contain threats in real time through automated quarantine and other mitigation features.

Threat intelligence

Cloud App Security correlates attack campaigns across diverse industries and geographies. We draw on insight from Proofpoint Emerging Threats (ET) Intelligence, the timeliest and most accurate source of threat intel in the market. Our threat dashboard gives you visibility into:

- Who in your organisation is being targeted
- Who is attacking, and how
- What the attackers are after

Armed with this insight, you can easily tell the difference between broad-spectrum attacks and those that target executives and other high-value employees.

Cross-channel correlation

Cloud App Security correlates threat activity across email and cloud. That insight gives you visibility into at-risk users and security breaches. Through our dashboard, you can easily connect the dots between credential phishing email attacks and suspicious logins. This insight helps you prioritise users most at risk. You can monitor these cloud accounts more closely or protect them with stricter access-control policies to defend against account compromise.

Top User at Risk
Last 30 days

User	Suspicious Logins	Failed Logins Attemps	Email Threats	Phishing Threats	Permitted Clicks	Last User Activity
Joe Greene Jgreene@acme.com	14	0	0	0	0	Jul 10 12:47 PM
Abby Boyle aboyle@acme.com	12	0	0	0	0	Jul 04 12:33 PM

Cloud App Security helps correlate user activity and contextual risk

MONITOR AND CONTROL CLOUD ACCESS

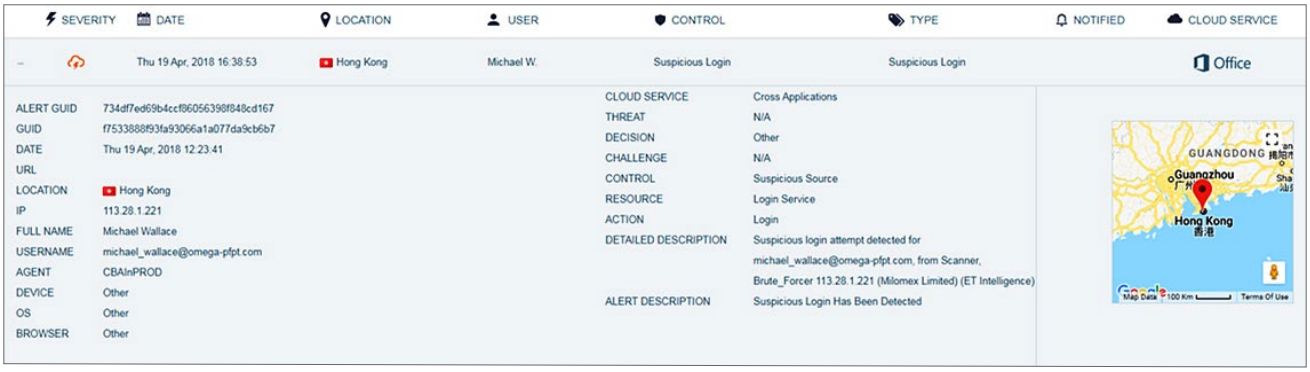
Today's workforce demands anytime, anywhere, any-device access to the cloud. In this environment, monitoring user behaviours across cloud apps is critical. This effort starts with establishing safe, baseline behaviours. Anomalous user behaviours may indicate that attackers have:

- Compromised users' accounts
- Stolen information
- Destroyed data

Based on risk indicators, you can act right away. Create policies to control access to cloud services. Enforce user validation through multi-factor authentication. Our powerful behaviour analytics, combined with strong authentication, helps you verify users' identity. That helps you grant the right levels of access to users and third-party add-ons.

Behavioural analytics

Cloud App Security brings together contextual data and user behaviour analytics. Context includes a user's location, device, network and any cloud app the user is trying to access. Anomalous behaviour includes excessive activities, unusual access attempts and more.



We monitor anomalies using captured footprints, thresholds and advanced machine learning. For example, you can:

- Specify that only corporate devices that meet your endpoint security standards can access a given cloud app
- Limit permissions with read-only access
- Limit the data that the user can download

Cloud App Security correlates cross-channel threat intelligence with user-specific risk indicators. With this insight, you can detect suspicious activity early, prioritise alerts and ease alert fatigue. You can also audit past activity and alerts through our intuitive dashboards and filtering. With our robust policy templates, you can get real time alerts. From there you can apply risk-based authentication and reduce privileges when needed. That prevents your apps from being misused—and your data from being exposed or deleted.

Multi-factor authentication

You can integrate existing identity-management solutions using our SAML proxy. Our multi-factor authentication also verifies user identities before login or other risky activity. With our multimode architecture, you can enable protection through API or by forward and reverse proxy.

CLOUD APP SECURITY HELPS YOU SECURE

CLOUD EMAIL

- Office 365 Exchange Online
- Gmail

CLOUD SERVICES

- Office 365 Exchange Online (Data-at-rest)
- Office 365 SharePoint Online
- Office 365 OneDrive
- Google Drive
- Google Cloud
- Box
- Dropbox
- Salesforce
- Amazon Web Services S3

PREVENT DATA LOSS IN THE CLOUD

As more of your organisation's data is stored in the cloud, so is sensitive content. Half of data breaches reported are a result of stolen or weak login credentials. Credentials are often compromised through data breaches, phishing, credential stealers and brute force attacks. To detect and prevent data breaches in the cloud, you need risk-aware data security and strong authentication.

Cloud App Security blends cross-channel threat detection with sensitive data visualisation and DLP controls. User-centred visibility and behaviour monitoring quickly reveals people being targeted and activity on orphaned and compromised accounts. Proofpoint DLP scans the following to highlight who has access to sensitive data:

- Emails in motion
- Emails at rest
- Cloud storage
- Data stored by other cloud apps

With this information, you can quickly prioritise which users need protection. From there, you can minimise sensitive data loss and contain any damage. Data-security rules can automatically encrypt emails, reduce file access permissions, and trigger multi-factor authentication for users at risk.

Data loss prevention

Proofpoint DLP has more than 80 predefined data security policies. You can automatically detect and classify sensitive data. You can also remediate DLP violations in cloud-based email and apps to help you identify and secure sensitive data faster. Our capabilities include:

- Unified data classifiers track data in motion and at rest.
- Built-in classifiers cover PCI, PII, HIPAA and GDPR regulations.
- Dictionaries and proximity matching improve detection of sensitive data and automate regulatory compliance.
- Exact data matching easily uploads custom dictionaries or identifiers to detect information unique to your organisation. This includes account numbers and other structured data from databases.
- Document fingerprinting detects sensitive data within unstructured content. These include formulas, source code, forms, contracts and other intellectual property.
- We scan 300 file types out of the box. Our file-type profiler extends support to new, custom or proprietary file types.

Flexible custom rules allow you to build your own DLP policies to control how your data is sent, shared and downloaded. You can control risky or unauthorised access to email and files to mitigate open sharing with context-aware encryption, quarantines and file-sharing permissions. And you can closely monitor compliance by subscribing to alerts and filter events and alerts for reporting.

AUTOMATE THIRD-PARTY APPS CONTROLS

Cloud app marketplaces offer hundreds of third-party add-ons that can enhance Microsoft Office 365, Google G Suite, Box and other platforms. The sheer variety of these ecosystems has made third-party access to your data a huge compliance risk.

Some email and file editing add-ons request full access to email, contacts and file content. They may also store this data in multiple geographies, possibly violating PII and GDPR regulations.

Our deep, vendor-neutral assessment safeguards against third-party add-on apps and scripts. We help you keep users productive and limit their risk with the right level of visibility and control. Alerts inform you of newly added risky apps and scripts. Controls allow you to define or automate actions based on analysis results and the app's risk score. Policies help define permissions granted for an access token. They can also deny an OAuth access request from an app or script that exceeds defined thresholds.

DEPLOY QUICKLY IN THE CLOUD

Cloud-based platforms need cloud-based protection. Our cloud architecture enables you to deploy quickly and derive value right away. You can protect hundreds of thousands of users in days—not weeks or months. We use the cloud to update our software every day with new features and help you stay ahead of attackers. Our cloud-based deployment also gives you the flexibility to protect users on any network or device.

PRODUCTS

Proofpoint Targeted Attack Protection (TAP) detects, analyses, and blocks advanced threats that target people through email (TAP for Email) and cloud apps (TAP SaaS Defence). We detect known threats and new, never-before-seen attacks that use malicious files and unsafe URLs. TAP is unmatched in stopping targeted attacks that use polymorphic malware, weaponised documents and credential-stealing phishing techniques to access sensitive information. Learn more at proofpoint.com/uk/product-family/advanced-threat-protection.

Proofpoint Cloud App Security Broker (PCASB) protects users of cloud apps from advanced threats, unauthorised access, data loss and compliance risks. PCASB provides a granular people-centric view of app access and data handling. Our solution combines advanced threat protection, access control, data loss prevention (DLP), third-party apps governance and multi-factor authentication to help you secure Microsoft Office 365, Google G Suite, Box and more. Our powerful analytics help you grant the right levels of access to users and third-party apps based on the risk factors that matter to you. Learn more and sign up for a free risk assessment at proofpoint.com/uk/products/cloud-app-security-broker.

Proofpoint Email Data Loss Prevention and Encryption prevents sensitive data loss through email and secures sensitive emails and attachments via automatic classification and policy-based encryption without the complexity and costs of legacy solutions. Learn more at proofpoint.com/uk/product-family/information-protection.